An associative block design ABD(10,5) does not exist

AN ASSOCIATIVE BLOCK DESIGN ABD(10,5) DOES NOT EXIST

by

J.A. La Poutré and J.H. van Lint

ABSTRACT: We prove the nonexistence of an ABD(10,5).

1. INTRODUCTION

So-called *associative block designs* were introduced by Rivest [4] in connection with the study of generalized hash-coding algorithms for performing partial-match searches of a random-access file of binary words. They also allow an interpretation as a special kind of packing of the k-dimensional affine space AG(k,2) with (k - w)-flats. The definition is as follows:

DEFINITION 1.

Let k and w be integers, $0 \leqslant w \leqslant k$, $k > 0$. An ABD(k,w) is a rectangular array, with $b = 2^w$ rows and k columns, with entries from {0,1,*}, such that:

(i) each row has w digits and (k - w) stars,

(ii) each column contains the same number $\frac{b(k-w)}{k}$ of stars,

(iii) the rows represent disjoint subsets of $\{0,1\}^k$, where a row is said to represent the subset of $\{0,1\}^k$ obtained by replacing the stars in all possible ways by zeros and ones.

That is, given any two rows, there is a column in which they contain different digits.

[So, every vector in $\{0,1\}^k$ is represented by a unique row of the ABD].

If we consider the rows of the ABD(k,w) as words in $\{0,1,*\}^k$ and if we modify Hamming distance by specifying that a * does not contribute to the distance, then (iii) above states that any two rows have distance at least 1. As usual, the number of ones in a row is called the *weight* of the row.

A number of construction methods for ABD's and several nonexistence theorems were found about ten years ago. These can be found in a paper by Brouwer [1] and in a survey by Van Lint [3]. The theorems which we shall need will be quoted below. As far as we know no new results were found until 1985. In [2] La Poutré proved Theorem 3, given below. An attempt to prove the nonexistence of an ABD(10,5) led to a partial result, which was mentioned without proof in [1]. We shall give a proof of this in Section 2 and then we shall complete the nonexistence proof of this design. In fact, we found two different (but similar) proofs. In both a not very elegant though elementary calculation is necessary. So we give only one of these proofs.

One of the tools which we need in our proofs is a simple consequence of Definition 1 (iii).

LEMMA 1. Let S be a subset of the columns of an ABD(k,w).
A row of the design is called *even* (resp. *odd*) with respect to S if it has digits in every column of S and among these an even (resp. odd) number of ones. Then there are as many even rows as odd rows.

Proof: A row which has one or more stars in S represents as many elements of $\{0,1\}^k$ with even weight in S as elements with odd weight in S. Definition 1 (iii) makes the assertion obvious. ∎

From [4], [1] and [2] we quote the following theorems.

THEOREM 1. *If an* ABD(k,w) *exists, then it has exactly* bw/(2k) *zeros and* bw/(2k) *ones in each column.*

If two rows have stars in the same position, then we shall say they have the same *star-pattern.*

THEOREM 2. *If an* ABD(k,w) *exists and* $w > 0$, *then*

(i) *a given star-pattern occurs in an even number of rows,*

(ii) *among the rows with a given star-pattern, as many have even weight as odd weight.*

If two rows have the same star-pattern, we shall call them a *row pair.*

THEOREM 3. *If an* ABD(k,w) *exists and* $w > 3$, *then* $k \leq \binom{w}{2}$.

Note that for k = 10, w = 5, we have equality in Theorem 3.

The aim of this note is to prove that an ABD(10,5) does not exist. As far as we know this is the only nonexistence result presently known, which is not an immediate consequence of the nonexistence theorems mentioned above.

NOTATION: In the following R will denote $\{0,1\}^{10}$, we assume that an ABD(10,5) exists and call it B. The row 0^5*^5 means the row starting with five zeros followed by five stars. If we are interested in the positions of a subset S of B, then a row will be said to have *type* $a^{\ell}b^{m}*^{n}$, if it has ℓ symbols a, m symbols b and n stars in these positions, where (a,b) is (0,1) or (1,0).

In [1] Brouwer mentions that $\mathcal{B}$ cannot have a row pair with distance 5. We give a proof in Section 2. In Section 3 we show that $\mathcal{B}$ cannot have a row pair with distance 3. In Section 4 it is shown that in fact $\mathcal{B}$ does not exist.

2. NO ROW PAIR HAS DISTANCE 5

Assume that 0^5*^5 and 1^5*^5 are the first two rows of $\mathcal{B}$. Let S denote the first five columns of $\mathcal{B}$. By Definition 1-(iii) each of the remaining 30 rows has at least one 0 and one 1 in S. We can split these rows into α rows of type $ab*^3$, β rows of type a^2b*^2, γ rows of type a^2b^2*, δ rows of type ab^3*, ρ rows of type ab^4 and σ rows of type a^2b^3. Hence

$$\alpha + \beta + \gamma + \delta + \rho + \sigma = 30. \tag{2.1}$$

By Definition 1-(ii) there are 80 digits in S. Hence

$$2\alpha + 3\beta + 4\gamma + 4\delta + 5\rho + 5\sigma = 70. \tag{2.2}$$

We now apply Theorem 2-(ii) to each pair of columns from S and then add the even weight count and the odd weight count. Since the results must be equal, we find

$$\alpha + \beta + 2\gamma - 2\rho + 2\sigma = 20. \tag{2.3}$$

Adding (2.2) and (2.3) and then subtracting three times (2.1) yields

$$\beta + 3\gamma + \delta + 4\sigma = 0,$$

after which we can solve for α and ρ. This yields $\rho = 10/3$ which is absurd. This establishes Lemma 2.

LEMMA 2. No row pair in $\mathcal{B}$ has distance 5.

Similar counting arguments (slightly more complicated) will be used in the next section.

3. NO ROW PAIR HAS DISTANCE 3

Assume that $\mathcal{B}$ has 0^5*^5 as its first row and $1^3 0^2 *^5$ as second row. Let A denote the first three columns and B the next two columns. We order the rows of $\mathcal{B}$ as follows. The first two from the set I. The rows of the set II do not have a 1 in B, the rows of the set III do. We use r(II) and r(III) for the number of rows of II resp. III. From Theorem 1 we have

(3.1) $\quad r(III) \leqslant 16.$

In the following figure we indicate the different types of rows which are possible in II and III and introduce symbols for the number of rows of each type.

	A	B	number
I	0 0 0	0 0	1
	1 1 1	0 0	1
II	a b b		t_1
	a b *		t_2
III	a a a		m
	a a *		n
	a b b		α
	a b *		β
	a * *		γ
	* * *		δ

By definition we have

$$(3.2)\qquad \begin{cases} r(II) = t_1 + t_2 , \\ r(III) = m + n + \alpha + \beta + \gamma + \delta , \\ r(II) + r(III) = 30 . \end{cases}$$

In the following, m_0 denotes the number of rows in III of type 000, and similarly for m_1, n_0, etc.

Counting digits in A we find (using Def.1-(ii))

$$(3.3)\qquad 48 = 6 + (3t_1 + 2t_2) + (3m + 2n) + (3\alpha + 2\beta + \gamma).$$

Now, (using Def. 1-(iii)) we count the represented vectors in $\mathcal{R}$ with 000 resp. 111 in A. We find

$$2^7 = 2^5 + 2^5 m_i + 2^4 n_i + 2^3 \gamma_i + 2^2 \delta \qquad (i = 0,1) ,$$

i.e.

$$(3.4)\qquad 24 = 8m_i + 4n_i + 2\gamma_i + \delta , \qquad (i = 0,1).$$

This implies

$$(3.5)\qquad 24 = 4m + 2n + \gamma + \delta .$$

From (3.2) and (3.5) we find the relation

$$(3.6)\qquad 3m + n + 6 = r(II) + \alpha + \beta .$$

LEMMA 3. $r(II) \leqslant 15$.

Proof: Suppose $r(II) \geqslant 16$. Then from (3.6) we find $3m + n \geqslant 10$. However, (3.3) implies $3m + 2n \leqslant 42 - 2r(II) \leqslant 10$. Therefore $3m = 10$, which is absurd. ∎

LEMMA 4. r(II) = 14. [So, every row in III has exactly one 1 in B].

Proof: By (3.1), (3.2) and Lemma 3 it suffices to prove r(II) $\neq$ 15. So, suppose r(II) = 15. As before we find from (3.3) and (3.6)

$$3m + n = 9 + \alpha + \beta ,$$

$$3m + 2n \leqslant 12 - (3\alpha + 2\beta + \gamma) .$$

It follows that $\alpha = 0$, $\beta \leqslant 1$. If $\beta = 1$, we again find $3m = 10$. So, $\beta = 0$. We are left with two solutions for m and n, namely $m = 3$, $n = 0$ (which implies $\gamma = 3$) and $m = 2$, $n = 3$ (and $\gamma = 0$, $\delta = 10$). The first of these is impossible since γ is even, by Theorem 2-(i). To exclude the second solution we substitute $\gamma = 0$, $\delta = 10$ in (3.4). ∎

LEMMA 5. We must have m = n = 2.

Proof: We have shown that r(II) = 14, r(III) = 16. We argue as in the previous lemmas. From (3.3), (3.5), (3.6) we find

$$(3.7) \qquad \begin{cases} 14 = t_1 + (3m+2n) + (3\alpha+2\beta+\gamma) , \\ 24 = \quad (4m+2n) + (\gamma+\delta) , \\ 8+\alpha+\beta = \quad (3m+n) . \end{cases}$$

The first and third of these yield

$$(3.8) \qquad 6 = t_1 + n + (4\alpha + 3\beta + \gamma).$$

We observe that γ and δ are even by Theorem 2-(i). Furthermore, it follows from (3.4) that if $\delta \geqslant 10$ then $m_i \leqslant 1$, so $m \leqslant 2$. However, (3.8) and the third equation in (3.7) show that $m > 2$ implies $m = 3$, $\alpha + \beta = 1$, $n = 0$ and $\gamma \leqslant 2$. Then the second equation in (3.7) yields $\delta \geqslant 10$, a contradiction. So $\alpha = \beta = 0$, $m = n = 2$ or $m = 1$, $n = 5$ or $\alpha = 0$, $\beta = 1$, $m = 2$, $n = 3$. The latter possibilities lead to $\gamma = 0$, $\delta = 10$, which again contradicts (3.4). ∎

LEMMA 6. At least one of the rows of type aaa in III has $\{0,1\}$ in B.

Proof: From Lemma 4 we know that each of the two rows of type aaa in III has one 1 in B. So it suffices to show that the other element in B is not a star. Suppose both type aaa rows of III have a star in B. We apply Lemma 1 to each of the three sets of four columns obtained by taking two columns from A and the two columns of B. We add the results. First, observe that the even count has a contribution of 6 from I. So, the remaining rows must contribute 6 more to the odd count than to the even count. This surplus can only be achieved by rows from II with 00 in B and possibly the two rows of type aa* in III. It follows that at least four rows of II have 00 in B. Since we now have at least six rows with 00 in B, Lemma 1 implies that six rows of III have a 0 in B. This yields 18 zeros in B, contradicting Theorem 1. ∎

From Lemma 6 we know that there is a row in III starting with 000 01 (w.l.o.g.). The remaining seven rows of III which have a 1 in the fifth column, must each have a 1 in A. From the proof of Lemma 5 we know that $m = 2$, $n = 2$, $\gamma \leqslant 4$. Therefore $\gamma = 4$ and these seven rows have a total of 11 ones. Together with the rows of I and II this gives us at least 28 ones in A, contradicting Theorem 1. This establishes the main result of this section.

LEMMA 7. A row pair with distance 3 does not exist.

4. NONEXISTENCE OF AN ABD(10,5)

From Lemma 2, Lemma 7, and Theorem 2 we can now conclude that $\mathcal{B}$ consists of 16 row pairs, each with distance 1. Let $\mathcal{B}$ have $r_0 = 0^5 *^5$ and $r_1 = 0^4 1 *^5$ as the first two rows. We represent this row pair as $0^4 - *^5$ using the

notation of [1].

Let A denote the first four columns of $\mathcal{B}$. Since both r_0 and r_1 are even in A, it follows from Lemma 1 that these must be compensated by odd rows. A row pair (r_2,r_3) only contributes to this compensation if both rows are odd in A. It follows that the digit in which they differ is not in A. Let (r_2,r_3) be such a row pair. The remaining 28 rows have at least 28 ones in A by Definition 1-(iii). Since there are 32 ones in A, it follows that r_2 and r_3 each have one 1 in A. So, w.l.o.g. the pair (r_2,r_3) is represented by $0^3 1 - **^4$ or by $0^3 1 * - *^4$. Now consider the first three columns. As before, we see that there must be at least 28 ones in these columns and the remaining rows, which contradicts Theorem 1. This establishes our main result.

THEOREM 4. An ABD(10,5) does not exist.

REFERENCES

[1] A.E. Brouwer, On associative block designs. In Colloquia Mathematica Societatis János Bolyai 18, Combinatorics, 173 - 184.

[2] J.A. La Poutré, A theorem on associative block designs, Discrete Mathematics (to appear).

[3] J.H. van Lint, {0,1,*} distance problems in combinatorics, in Surveys in Combinatorics 1985 (I. Anderson, ed.), L.M.S. Lecture Note Series 103, Cambridge Univ. Press., 113 - 135.

[4] R.L. Rivest, On hash-coding algorithms for partial-match retrieval. Proc. of the 15-th Annual Symposium on Switching and Automata Theory, 95 - 103.